

Bibliographic data: CN 1384639 (A)

Distributed dynamic network security protecting system

Publication date: 2002-12-11
Inventor(s): HAN ZONGFEN [CN]; JIN HAI [CN]; LIU KE [CN] +
Applicant(s): UNIV HUAZHONG SCIENCE TECH [CN] +
Classification:
- **international:** **H04L9/00;** (IPC1-7): H04L9/00
- **European:**
Application number: CN20021015957 20020611
Priority number(s): CN20021015957 20020611
Also published as: • CN 1160889 (C)

Abstract of CN 1384639 (A)

The distributed dynamic network security protecting system has central network administration station provided with summarizing decision module and policy releasing module. The network is divided into N subnetworks in tree structure, and each subnetwork administration station is provided with summarizing decision module and policy releasing module. Each node in the subnetwork has micro invasion detecting module and micro fire wall module installed. In the policy releasing module, mobile agency technology is adopted. The distributed micro invasion detecting module provides security protection in application layer while the distributed micro fire wall module provides security protection in kernel level. The double security protection makes the system capable of preventing outer and inner attack, preventing cooperative invasion and providing dynamic immunity.

[12] 发明专利申请公开说明书

[21] 申请号 02115957.2

[43] 公开日 2002 年 12 月 11 日

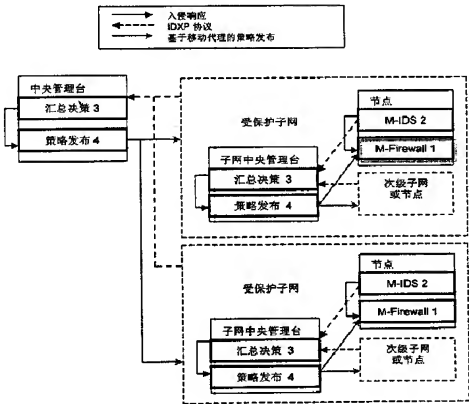
[11] 公开号 CN 1384639A

<div>[22] 申请日 2002.6.11 [21] 申请号 02115957.2</div> <div>[71] 申请人 华中科技大学</div> <div>地址 430074 湖北省武汉市洪山区珞喻路 1037 号</div> <div>[72] 发明人 韩宗芬 金海 刘科 鲜丰 易川江 孙建华 郭立</div>	<div>[74] 专利代理机构 华中科技大学专利中心</div> <div>代理人 方放</div>
权利要求书 4 页 说明书 12 页 附图 4 页	

[54] 发明名称 分布式网络动态安全保护系统

[57] 摘要

本发明的分布式网络安全保护系统,网络中央管理台配置汇总决策模块和策略发布模块,网络按照树型结构分为 N 个子网,各子网管理台上均配置汇总决策模块和策略发布模块,子网中每个节点都安装微入侵检测模块和微防火墙模块,策略发布模块采用移动代理技术;本系统的分布式微入侵检测模块可提供应用层的安全保护,分布式微防火墙模块提供内核级的网络层安全保护,不仅以网段为保护单位,而且还以单个节点机为保护对象,从而实现双重细粒度的安全保护;该系统与传统的入侵检测和防火墙产品相比,具有防止外部和内部攻击、可扩展性强、防单失效点、防范协同入侵、实时安全保护及动态自免疫等优点。



1、一种分布式网络动态安全保护系统，网络中央管理台配置汇总决策模块和策略发布模块，网络按照树型结构分成 N 个子网， $N \geq 1$ ，各子网管理台上均配置汇总决策模块和策略发布模块，子网中每个节点都安装微入侵检测模块和微防火墙模块，

子网各节点的微防火墙模块用于接收网络数据包、丢弃非法数据包，将合法数据包传送给同一节点的微入侵检测模块；

入侵检测模块用于检测数据包，若发生常规入侵则修改微防火墙模块的安全策略，否则将安全事件传送给本子网的微汇总决策模块；

各子网的汇总决策模块根据本子网各节点发送的当前安全事件检测协同入侵，并根据其严重程度判决是否需要传给上级管理台，若不传给上级管理台，则通知策略发布模块，启动子网移动代理系统，登陆到本子网各节点修改微防火墙模块的安全策略；

中央管理台汇总决策模块接收各子网汇总决策模块发来的协同入侵事件，并通知策略发布模块生成全局安全策略，策略发布模块启动全局移动代理系统，把策略发送到各子网管理台的策略发布模块，从而修改所有节点微防火墙模块的安全策略。

2、如权利要求 1 所述的分布式网络动态安全保护系统，其特征在于各个子网可以进一步划分为若干次级子网。

3、如权利要求 1 或 2 所述的分布式网络动态安全保护系统，其特征在于：

- (1) 微防火墙模块包括包过滤模块和包过滤策略库，包过滤策略库定义当前安全策略，包过滤模块驻留于网络协议层，它根据包过滤策略库对所有流经网络协议层的数据包进行过滤，丢弃非法数据包，将合法数据包提交微入侵检测模块；
- (2) 微入侵检测模块包括事件采集器、常规安全事件库、常规入侵规则库、常规入侵分析器和常规入侵响应器，事件采集器实时采集包过滤模块传送的数据包，并按预定格式组合成网络安全事件存入常规安全事件库，同时发送给常规入侵分析器和汇总决策模块，常规入侵规则库存放描述常规入侵的规则，常规入侵分析器将这些规则转换为规则链表并将发送来的网络安全事件与其遍历匹配，当产生一个完全匹配时，通知常规入侵响应器，同时修改包过滤策略库；
- (3) 汇总决策模块包括事件接收模块、协同安全事件生成模块、抽象化模块、支持度和可信度计算模块、阈值比较模块、协同事件数据库、协同入侵分析器和协同入侵规则库，事件接收模块接收微入侵检测模块的事件采集器发来的网络安全事件，存入协同事件数据库，同时通过协同安全事件生成模块产生协同安全事件，并传给抽象化模块，该模块将协同安全事件诸字节抽象化为一个取值范围，并作为候选的新协同入侵规则 Y 传给支持度和可信度计算模块，后一模块遍历协同入侵规则库中每条安

全规则 X 计算 X 与 Y 关联的支持度和可信度，并将其传给阈值比较模块，与预先定义的最小支持度阈值和最小可信度阈值分别比较，若都有大于阈值，则将 Y 存入协同入侵规则库中，协同入侵分析器根据协同事件数据库和协同入侵规则库判别协同入侵事件的类型并给出相应的安全策略，传给策略发布模块；

- (4) 子网/全局移动代理系统由驻留于子网/中央管理台的移动代理客户端和驻留于各节点/子网管理台的移动代理服务器端组成，移动代理客户端包括用户界面、签名模块、代理路线记录模块和客户端代理传输协议栈，用户界面定义移动代理的数字签名算法类型并提交给签名模块，同时定义代理路线记录模块的相关内容，签名模块对移动代理进行数字签名供各节点/子网策略发布模块验证，代理路线记录模块保存移动代理将要周游的节点/子网管理平台序列，并通过客户端代理传输协议栈与服务器交互；移动代理服务器端包括服务器端代理传输协议栈、代理资源控制模块、合法性检查模块和策略解释器，客户端和服务器的代理传输协议栈提供客户端/服务器端的底层信息交互机制，代理资源控制模块为移动代理提供执行环境，合法性检查模块验证移动代理的数字签名，并把代理携带的安全策略传给策略解释器，然后将安全策略解释为策略脚本并加载到微防火墙模块的包过滤策略库中。

4、如权利要求 3 所述的分布式网络动态安全保护系统，其特征在于：

- (1) 微防火墙模块还包括策略定义用户界面和策略沙盒模块，策略定义用户界面支持用户自定义安全策略规则并将其传给策略沙盒模块，然后将用户自定义安全策略规则与包过滤策略库中的安全策略规则进行比较，若发现冲突则丢弃该用户自定义的安全策略规则，否则存入包过滤策略库中；
- (2) 汇总决策模块还包括规则淘汰模块和定时器，规则淘汰模块对新协同入侵规则 Y 定义使用频度，每当 Y 支持一个抽象协同入侵事件，该规则的使用频度加 1，当协同入侵规则库中生成的协同入侵规则数到达最大时，该模块采用最近最少使用算法淘汰使用频度低的规则；定时器定时给规则淘汰模块发信号，以便淘汰最少使用的入侵规则。
- 5、如权利要求 3 所述的分布式网络动态安全保护系统，其特征在于所述协同安全事件为一组彼此相关的网络安全事件集，它们可以在时间上相关，即按发生时间排序，相邻两个事件间隔不超过规定单位时间；也可以在空间上相关，即构成此协同安全事件的网络安全事件的源网络协议地址来自同一子网。
- 6、如权利要求 4 所述的分布式网络动态安全保护系统，其特征在于所述协同安全事件为一组彼此相关的网络安全事件集，它们可以在时间上相关，即按发生时间排序，相邻两个事件间隔不超过规定单位时间；也可以在空间上相关，即构成此协同安全事件的网络安全事件的源网络协议地址来自同一子网。

分布式网络动态安全保护系统

技术领域

本发明属于计算机安全领域，具体涉及一种基于分布式微防火墙和微入侵检测的网络动态安全保护系统。

背景技术

随着网络犯罪的递增和黑客网站的涌现，网络安全成为计算机及其应用领域至关重要的问题，因此网络安全工具层出不穷。虽然人们对网络协议不断修改，但是备受瞩目的当属网络安全工具中比较成熟和早已产品化的入侵检测和防火墙技术。这两项技术是建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，目标是保护数据、资源和用户的声誉。

中国网络安全响应中心的技术报告指出，当前的入侵检测系统面临两个主要挑战：一个是虚警率太高，美国政府利用国家科学基金会的资金资助学术界对虚警问题的研究，足见问题之严重；另一个是检测速度太慢，目前大多数入侵检测系统在不牺牲检测质量的前提下尚不能处理百兆位网络满负荷时的数据量。

1999年，S. M. Bellovin 在《login:》杂志 24 卷第 5 期上发表的“Distributed Firewalls”首次提出分布式防火墙的结构，其示意图如图 1 所示。该结构在受保护子网的各个节点上安装防火墙进行数据包的访问控制，同时中央管理台对防火墙的安全策略进行集中管理，并由策略发布模块将安全策略发布到各个防火墙上，发布机制采用 TFTP (Trivial File Transfer Protocol, 简单文件传输协议)。

该结构消除了传统防火墙存在的一些弱点（例如：依赖于网络的物理拓扑结构、不能防止内部攻击、效率不高、故障点多、无法有效地处理许多端到端的加密协议如 IPSec）。但是在该结构中，随着受保护节点的增加，中央管理台发布策略的任务将日趋繁重，降低了系统的可扩展性；另外，该结构不能防止日益严峻的协同式入侵行为，不能有效的实现动态自免疫。

发明内容

本发明针对现有入侵检测和防火墙技术的不足，提出一种分布式网络动态安全保护系统。本系统将分布式微入侵检测和微防火墙技术有机结合，在各个受保护的主机上安装微防火墙和微入侵检测系统，通过管理台的汇总决策和策略发布机制对入侵事件进行分析、关联、预警和处理，形成双层细粒度的安全保护，从而有效的防止了来自网络外部和内部的攻击，消除了防火墙的瓶颈效应，避免了单点失效，同时能防范分布式协同入侵、有效实现系统的动态自免疫和规模扩展。系统采用移动代理技术，能自主性的舒缓管理台的瓶颈效应，有效地防止策略管理台的单点失效，保证了系统具有良好的可扩展性。

从工作原理的角度可以将本系统分为两大部分，一是安装在受保护节点上的微防火墙系统和微入侵检测系统；二是安装在中央管理台上的 IDS 汇总决策模块和防火墙策略发布模块。

本发明分布式网络动态安全保护系统，网络中央管理台配置汇总决策模块和策略发布模块，网络按照树型结构分成 N 个子网， $N \geq 1$ ，各子网管理台上均配置汇总决策模块和策略发布模块，子网中每个节点都安装微入侵检测模块和微防火墙模块，

子网各节点的微防火墙模块用于接收网络数据包、丢弃非法数据包，将合

法数据包传送给同一节点的微入侵检测模块；

入侵检测模块用于检测数据包，若发生常规入侵则修改微防火墙模块的安全策略，否则将安全事件传送给本子网的微汇总决策模块；

各子网的汇总决策模块根据本子网各节点发送的当前安全事件检测协同入侵，并根据其严重程度判决是否需要传给上级管理台，若不传给上级管理台，则通知策略发布模块，启动子网移动代理系统，登陆到本子网各节点修改微防火墙模块的安全策略；

中央管理台汇总决策模块接收各子网汇总决策模块发来的协同入侵事件，并通知策略发布模块生成全局安全策略，策略发布模块启动全局移动代理系统，把策略发送到各子网管理台的策略发布模块，从而修改所有节点微防火墙模块的安全策略。

所述的分布式网络动态安全保护系统，各个子网可以进一步划分为若干级子网。

所述的分布式网络动态安全保护系统，其进一步的特征在于：

- (1) 微防火墙模块包括包过滤模块和包过滤策略库，包过滤策略库定义当前安全策略，包过滤模块驻留于网络协议层，它根据包过滤策略库对所有流经网络协议层的数据包进行过滤，丢弃非法数据包，将合法数据包提交微入侵检测模块；
- (2) 微入侵检测模块包括事件采集器、常规安全事件库、常规入侵规则库、常规入侵分析器和常规入侵响应器，事件采集器实时采集包过滤模块传送的数据包，并按预定格式组合成网络安全事件存入常规安全事件库，同时发送给常规入侵分析器和汇总决策模块，常规入侵规则库存

放描述常规入侵的规则，常规入侵分析器将这些规则转换为规则链表并将发送来的网络安全事件与其遍历匹配，当产生一个完全匹配时，通知常规入侵响应器，同时修改包过滤策略库；

- (3) 汇总决策模块包括事件接收模块、协同安全事件生成模块、抽象化模块、支持度和可信度计算模块、阈值比较模块、协同事件数据库、协同入侵分析器和协同入侵规则库，事件接收模块接收微入侵检测模块的事件采集器发来的网络安全事件，存入协同事件数据库，同时通过协同安全事件生成模块产生协同安全事件，并传给抽象化模块，该模块将协同安全事件诸字节抽象化为一个取值范围，并作为候选的新协同入侵规则 Y 传给支持度和可信度计算模块，后一模块遍历协同入侵规则库中每条安全规则 X 计算 X 与 Y 关联的支持度和可信度，并将其传给阈值比较模块，与预先定义的最小支持度阈值和最小可信度阈值分别比较，若都有大于阈值，则将 Y 存入协同入侵规则库中，协同入侵分析器根据协同事件数据库和协同入侵规则库判别协同入侵事件的类型并给出相应的安全策略，传给策略发布模块；

- (4) 子网/全局移动代理系统由驻留于子网/中央管理台的移动代理客户端和驻留于各节点/子网管理台的移动代理服务器端组成，移动代理客户端包括用户界面、签名模块、代理路线记录模块和客户端代理传输协议栈，用户界面定义移动代理的数字签名算法类型并提交给签名模块，同时定义代理路线记录模块的相关内容，签名模块对移动代理进行数字签名供各节点/子网策略发布模块验证，代理路线记录模块保存移动代理将要周游的节点/子网管理平台序列，并通过客户端代理传输协议栈

与服务器交互；移动代理服务器端包括服务器端代理传输协议栈、代理资源控制模块、合法性检查模块和策略解释器，客户端和服务端端的代理传输协议栈提供客户端/服务器端的底层信息交互机制，代理资源控制模块为移动代理提供执行环境，合法性检查模块验证移动代理的数字签名，并把代理携带的安全策略传给策略解释器，然后将安全策略解释为策略脚本并加载到微防火墙模块的包过滤策略库中。

所述的分布式网络动态安全保护系统，其更进一步的特征在于：

- (1) 微防火墙模块还包括策略定义用户界面和策略沙盒模块，策略定义用户界面支持用户自定义安全策略规则并将其传给策略沙盒模块，然后将用户自定义安全策略规则与包过滤策略库中的安全策略规则进行比较，若发现冲突则丢弃该用户自定义的安全策略规则，否则存入包过滤策略库中；
- (2) 汇总决策模块还包括规则淘汰模块和定时器，规则淘汰模块对新协同入侵规则 Y 定义使用频度，每当 Y 支持一个抽象协同入侵事件，该规则的使用频度加 1，当协同入侵规则库中生成的协同入侵规则数到达最大时，该模块采用最近最少使用算法淘汰使用频度低的规则；定时器定时给规则淘汰模块发信号，以便淘汰最少使用的入侵规则。

所述的分布式网络动态安全保护系统，其特征还可以在于所述协同安全事件为一组彼此相关的网络安全事件集，它们可以在时间上相关，即按发生时间排序，相邻两个事件间隔不超过规定单位时间；也可以在空间上相关，即构成此协同安全事件的网络安全事件的源网络协议地址来自同一子网。

本发明的分布式网络动态安全保护系统具有以下优点及效果。

1) 双重的安全保护

本系统包含两个相互平行的子系统：分布式微入侵检测模块（DM-IDS）可以提供应用层的安全保护；分布式微防火墙模块（DM-Firewall）提供内核级网络层的安全保护，从而提供双重的安全保护。

2) 细粒度安全保护

本系统不仅以网段为保护单位，而且还以单个节点机为保护对象，从而实现细粒度的安全保护。在各节点机上安装的微入侵检测系统(M-IDS)和微防火墙系统(M-Firewall)可以独立的检测和响应入侵，不仅消除了单一失效点，而且可以同时检测内部和外部攻击。

3) 树型可扩展架构

分层的树型管理模式使维护和管理易于扩展；移动代理自主移动的优点能够有效的节约网络带宽，从而使系统效率不会随受保护节点数目的增多而下降，达到系统效率的可扩展性；采用 JAVA 作为开发工具实现了平台无关性；

4) 动态自免疫

本系统将入侵行为分为常规入侵和协同入侵两种。微入侵检测收集各种安全事件，如果发现常规入侵，微入侵检测立即修改本节点微防火墙的策略，阻止入侵数据包的进一步涌入(常规入侵响应)；如果发现协同入侵，汇总决策模块通知策略发布机构向所有微防火墙发布更新策略（协同入侵响应）。两种响应使系统具有动态自免疫的功能；

5) 防御协同入侵

分布环境下的协同攻击与日俱增，传统的入侵检测技术已经不能满足应用

需求。本系统采用汇总决策技术对时间上和空间上分布的协同入侵行为进行汇总、关联和检测，并更新所有微防火墙的安全策略进行动态防御。

附图说明

图 1：现有分布式防火墙的体系结构。

图 2：基于分布式微防火墙和微入侵检测的分布式网络动态安全保护系统的体系结构。

图 3：本发明分布式网络动态安全保护系统流程示意图。

图 4：分布式微防火墙模块的结构及软件示意图。

图 5：分布式微入侵检测模块的结构及软件示意图。

图 6：汇总决策模块的结构及软件示意图。

图 7：移动代理模块的结构及软件示意图。

具体实施方式

在具有 16 个节点机上的集群系统构建一个基于分布式微防火墙和微入侵检测的网络动态安全系统，其基本配置如表 1 所示。

CPU	内存	硬盘	网卡	操作系统	网络
双 PIII 866	256M	30G	3C905B	Linux 6.2	100M 交换机

表 1 各节点的硬件及网络配置

其中，一台作为中央管理台，其余的服务节点按照服务分成若干组，如：Web 组、FTP 组。具体实施如下：节点 1 充当中央管理台，装载汇总决策模块和策略发布模块；节点 2 至节点 8 在 Web 组中，节点 9 至节点 16 在 FTP 组中，各节点上均装载微入侵检测模块和微防火墙模块。

结合附图，对整个系统的配置说明如下：

1) 包过滤策略库(8)

该策略库共 6 个字段，其示例如表 2 和表 3。

对 Web 组各节点（以 17.0.0.1 为例）的微防火墙具有类似表 2 的配置，对 FTP 组各节点（以 17.0.0.2 为例）的微防火墙具有类似表 3 的配置。

协议号	源 IP	源端口	目的 IP	目的端口	措施
TCP	10.0.0.1	>1024	17.0.0.1	80	ACCEPT
ANY	ANY	ANY	17.0.0.1	ANY	DROP

表 2 Web 组各节点的配置示例（以 17.0.0.1 为例）

协议号	源 IP	源端口	目的 IP	目的端口	措施
TCP	10.0.0.1	>1024	17.0.0.2	21	ACCEPT
ANY	ANY	ANY	17.0.0.2	ANY	DROP

表 3 FTP 组各节点的配置示例（以 17.0.0.2 为例）

各字段解释如下：

协议号：分为 TCP、UDP、ICMP、ANY，其中 ANY 指代任何协议；

源 IP：数据包的源 IP 地址；

源端口：数据包的源端口；

目的 IP：数据包的源 IP 地址；

目的端口：数据包的目的端口；

措施：指对匹配的数据包将存取何种措施，分为 ACCEPT（接收）和 DROP（拒绝）两种。

2) 常规安全事件库(10)

该事件库共 6 个字段，其示例如表 4。

协议号	源 IP	源端口	目的 IP	目的端口	时间
TCP	10.0.0.1	16666	17.0.0.1	80	2000.01.01.17.00
TCP	10.0.0.1	16667	17.0.0.1	80	2000.01.01.17.03

表 4 常规安全事件库示例

各字段的说明如下：

协议号：入侵事件的协议类型，分为 TCP、UDP、ICMP；

源 IP：入侵事件的源 IP 地址；

源端口：入侵事件的源端口；

目的 IP：入侵事件的源 IP 地址；

目的端口：入侵事件的目的端口；

时间：入侵事件发生的时间。

3) 常规入侵规则库(11)

该常规规则库共 5 个字段，其示例如表 5。

规则编号	攻击类型	攻击服务	攻击特征码	危害程度
1	Scan	ANY	“RST-ACK”	2
2	DoS	ANY	“SYN”	0

表 5 常规入侵规则库示例

各字段的说明如下：

规则编号：一条规则纪录的数字编号；

攻击类型：分为 Dictionary Attack（字典攻击）、Scan（端口扫描）、DoS（拒

绝服务攻击) 三种;

攻击服务: 各种众所周知的服务 (如 Web、FTP 等), ANY 表示任意服务;

攻击特征码: 表示代表一次攻击的标志性特征码;

入侵危害程度: 指入侵事件的危害程度, 该程度可分为: 最严重 (0 级)、较严重 (1 级) 和次严重 (2 级)。

4) 阈值比较器(18)

MinSupp 和 MinConf 的取值范围是大于 0 的整数。本实例中两个阈值设定如下: MinSupp=10, MinConf=10;

5) 协同事件数据库(19)

该数据库共 7 个字段, 其示例如表 6。

协同入侵 事件编号	相关性 (S/P)	入侵类 型	源 IP	目的 IP	入侵时间	入侵危 害程度
1	S	Scan	10.0.0.1	17.0.0.1	2000.01.01.17.00	2
1	S	DoS	10.0.0.1	17.0.0.2	2000.01.01.17.03	0

表 6 协同事件数据库的配置示例

各字段解释如下:

协同入侵事件编号: 指一组协同入侵事件的编号;

相关性: 分为空间相关 (S) 和时间相关 (T);

入侵类型: 分为 Dictionary Attack (字典攻击)、Scan (端口扫描)、DoS (拒绝服务攻击) 三种;

源 IP: 指入侵行为的源 IP 地址;

目的 IP：指被攻击的 IP 地址；

入侵时间：指入侵事件的发生时间；

入侵危害程度：指入侵事件的危害程度，该程度可分为：最严重（0 级）、较严重（1 级）和次严重（2 级）。

6) 协同入侵规则库(21)

该数据库共 6 个字段，其示例如表 7。

相关性 (S/P)	入侵类 型	空间相关度	时间相关度	入侵危 害程度	响应策略
S	Scan	>0.8	空值	2	断开
S	DoS	>0.5	空值	0	限流

表 7 协同入侵规则库的配置示例

各字段解释如下：

相关性：分为空间相关（S）和时间相关（T）；

入侵类型：分为 Dictionary Attack（字典攻击）、Scan（端口扫描）、DoS（拒绝服务攻击）三种；

空间相关度：当“相关性”字段为 S 时，此处为构成一次空间上分布的入侵行为的相关度范围；

时间相关度：当“相关性”字段为 T 时，此处为时间上分布的入侵行为的相关度；

入侵危害程度：指入侵事件的危害程度，该程度可分为：最严重（0 级）、较严重（1 级）和次严重（2 级）；

响应策略：针对某一协同入侵行为的全局响应策略。

7) 代理路线纪录(26)

该记录库共 2 个字段，保存代理的周游路线，该路线纪录以链表的形式保存在代理客户端的内存中，其初始值如表 8 所示。

组别	周游节点序列
Web	2, 3, 4, 5, 6, 7, 8
FTP	9, 10, 11, 12, 13, 14, 15, 16

表 8 代理路线纪录示例

该纪录表明移动代理将周游 Web 组的 2 到 8 节点和 FTP 组的 9 到 16 节点。

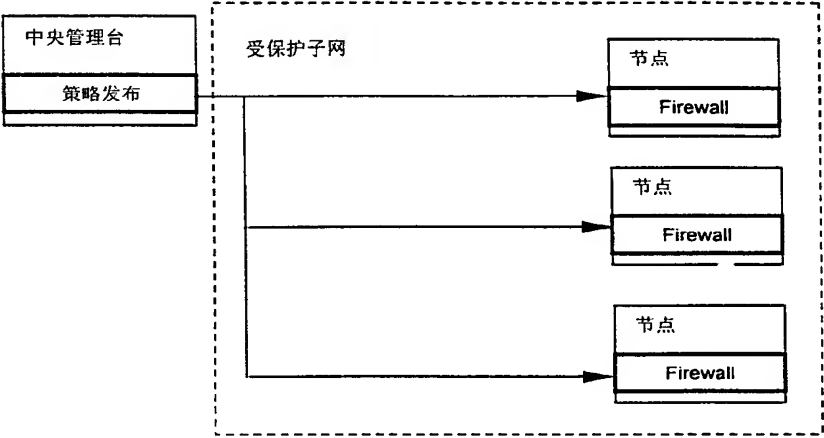


图 1

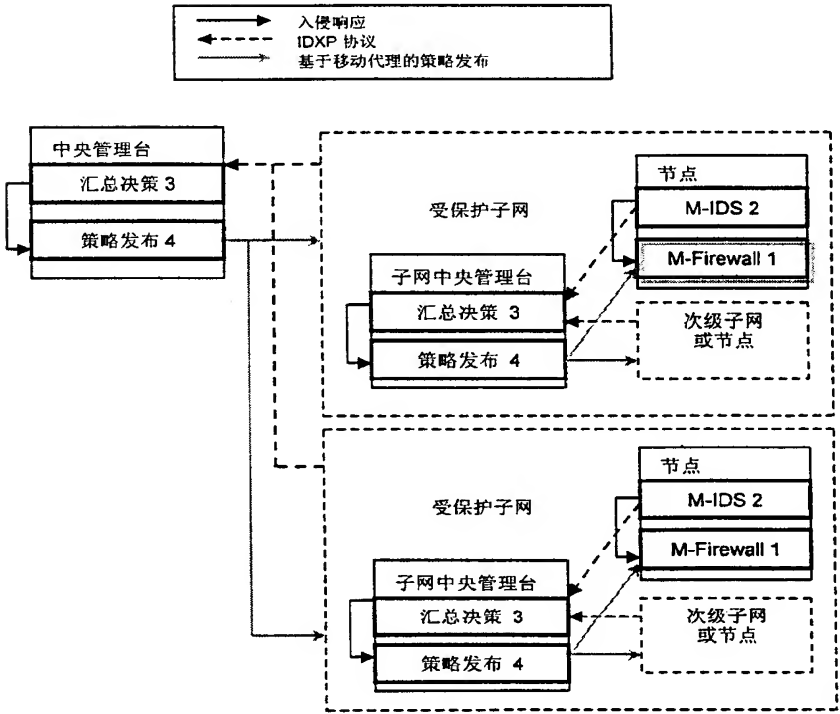


图 2

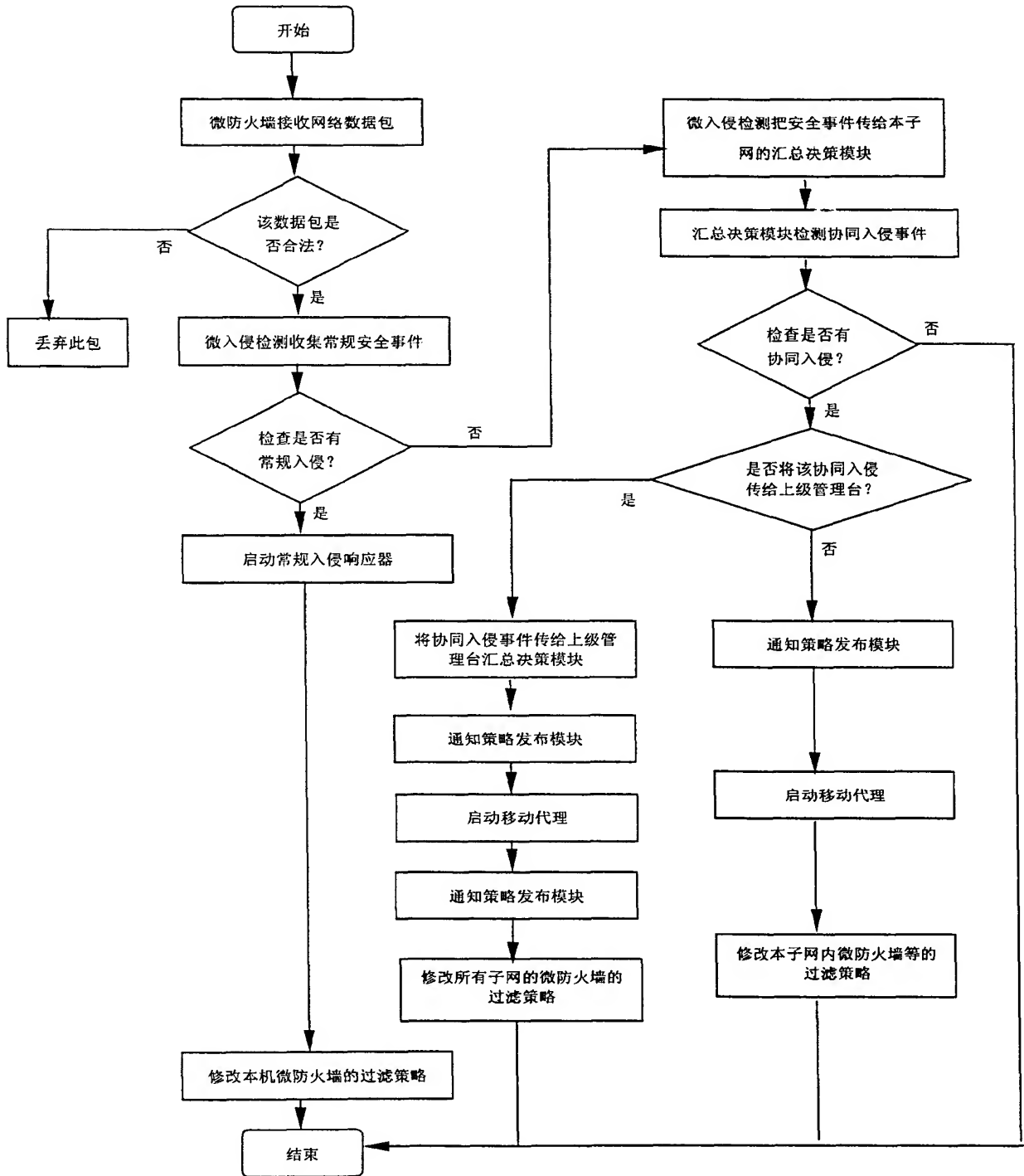


图 3

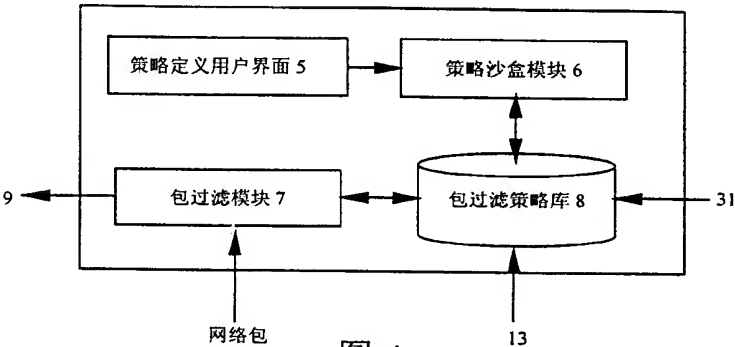


图 4

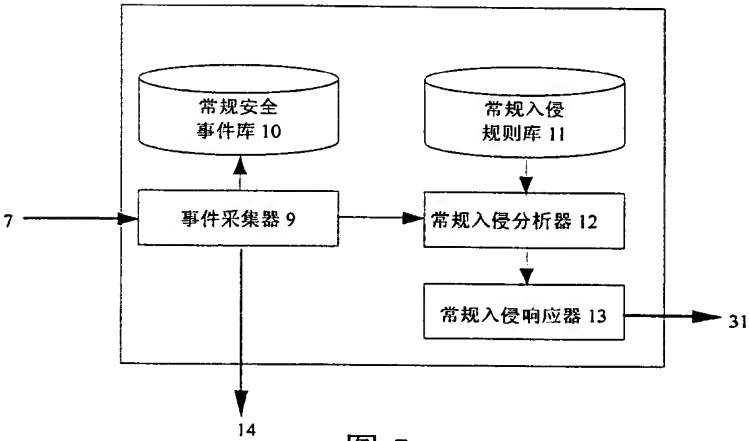


图 5

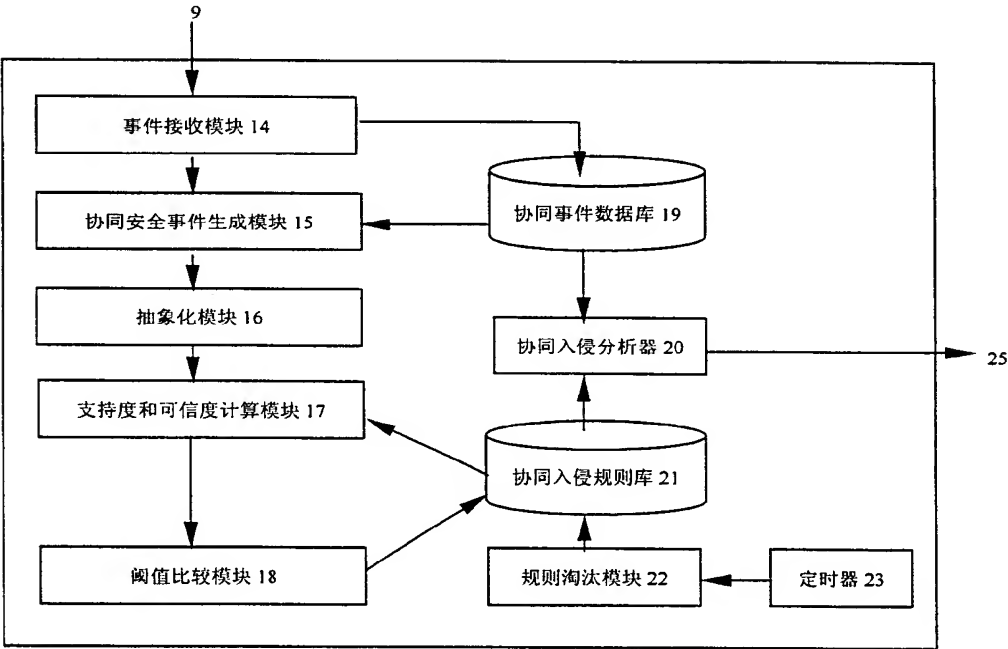


图 6

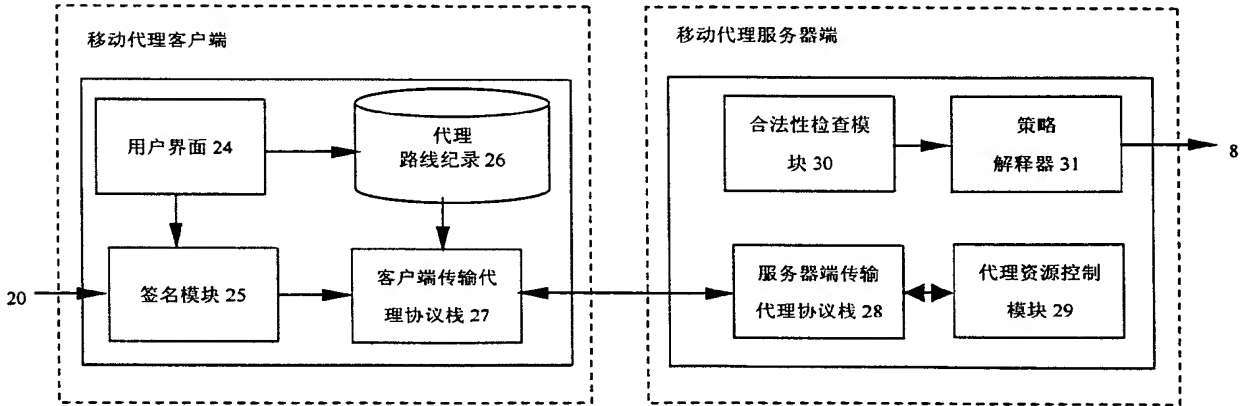


图 7